

Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare

☐ TLP:WHITE

Alert ID : 6e4fd0a5

Mar 23, 2023, 10:15 AM

This week, *Hacking Healthcare* examines the fallout of the 2020 Blackbaud ransomware incident that affected thousands of the organization's customers. Specifically, we examine what happened, how it led to a \$3 million regulatory settlement, and what Health-ISAC members can learn from it.

Welcome back to *Hacking Healthcare*.

March Monthly Threat Brief

Before we get to our main topic, and as we approach the end of March, we would like to remind all Health-ISAC members that the Monthly Threat Brief will be held on Tuesday the 28 at noon ET. The Threat Brief is one of the services provided by the Health-ISAC specifically for members, and features reports from Health-ISAC staff and Health-ISAC partners. Topics for this month include new trends in cybersecurity, emerging threats, cybercrime, physical security, and legal and regulatory developments.

Lessons From Blackbaud's SEC Order

Winding the clock back a bit, many of you may recall the Blackbaud ransomware incident that captured headlines back in 2020. Blackbaud is back in the news this month due to a \$3 million dollar settlement with the Securities and Exchange Commission (SEC) over how the company handled reporting of the incident. Despite Blackbaud itself not being a healthcare organization, there are important takeaways from the SEC settlement that can apply to Health-ISAC members, which we will summarize in the analysis section.

Let's begin with a brief recap of how this all started. Blackbaud is a U.S.-based entity that provides cloud software offerings to a variety of sectors including healthcare, education, and nonprofits. Back in May of 2020, Blackbaud was victimized by a ransomware attack that ultimately affected over 13,000 customers, including data from hundreds of thousands of individuals linked to healthcare entities.^[i]^[ii] Blackbaud ultimately paid a ransom demand and appeared to have believed that any data exfiltrated by the cybercriminal group responsible had been destroyed. They publicly stated that they had no reason to believe that customer data beyond names, addresses, and some contact information had been compromised.

Here is where Blackbaud appears to have gotten into trouble. The SEC notes in their order that days after publicly stating that the cybercriminals did not access bank account information or social security numbers, some Blackbaud personnel became aware that sensitive information actually had been accessed.^[iii] However, for undisclosed reasons, the personnel aware that sensitive customer information had been exposed reportedly did not inform the senior management responsible for handling disclosures.^[iv] This led to Blackbaud filing SEC forms in August that omitted these newly known facts, which then “misleadingly characterized the risk of exfiltration”.^[v] It wouldn’t be until the end of September that Blackbaud disclosed the full extent of the incident. The SEC further noted that Blackbaud “failed to maintain disclosure controls and procedures as defined in Exchange Act Rule 13a-15(e).^[vi]

As a result of these issues, the SEC found Blackbaud to have committed several violations of both the Securities Act and the Exchange Act and Rule. In total, Blackbaud has “agreed to pay \$3 million to settle charges for making misleading disclosures,” and has committed to avoiding any future violations.^[vii]

Action & Analysis

****Included with Health-ISAC Membership****

Congress

Tuesday, March 21st:

- No relevant hearings

Wednesday, March 22nd:

- No relevant meetings

Thursday, March 23rd:

- No relevant hearings

International Hearings/Meetings

- No relevant meetings

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

^[i] <https://techcrunch.com/2023/03/10/sec-blackbaud-charged-ransomware/>

^[ii] <https://healthitsecurity.com/news/blackbaud-ransomware-hack-affects-657k-maine-health-system-donors>

^[iii] <https://www.sec.gov/litigation/complaints/2023/comp-pr2023-48.pdf>

^[iv] <https://www.sec.gov/litigation/complaints/2023/comp-pr2023-48.pdf>

^[v] <https://www.sec.gov/litigation/complaints/2023/comp-pr2023-48.pdf>

^[vi] <https://www.sec.gov/litigation/complaints/2023/comp-pr2023-48.pdf>

^[vii] <https://www.sec.gov/news/press-release/2023-48>

^[viii] <https://www.sec.gov/litigation/complaints/2023/comp-pr2023-48.pdf>

^[ix] <https://www.sec.gov/litigation/complaints/2023/comp-pr2023-48.pdf>

^[x] <https://www.sec.gov/litigation/complaints/2023/comp-pr2023-48.pdf>

^[xi] <https://www.sec.gov/litigation/complaints/2023/comp-pr2023-48.pdf>

^[xii] <https://www.sec.gov/litigation/complaints/2023/comp-pr2023-48.pdf>

Reference | References

[Tech Crunch](#)

[Health IT Security](#)

[sec](#)

[Health-ISAC DDoS Whitepaper](#)

[sec](#)

[sec](#)

Report Source(s)

[Health-ISAC](#)

Tags

Regulatory, Incident Reporting, Hacking Healthcare, SEC, Incident Response, Securities And Exchange Commission, Ransomware

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Conferences, Webinars, and Summits:

<https://h-isac.org/events/>

Hacking Healthcare:

Written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.